УДК 004

А. А. Лысковец
курсант 2-го курса факультета милиции
Могилевского института МВД (Беларусь)

А. С. Мойсевич
преподаватель кафедры оперативно-розыскной деятельности факультета милиции
Могилевского института МВД
(Беларусь)

БЕЗОПАСНОСТЬ МОБИЛЬНОГО УСТРОЙСТВА

Мобильное устройство в настоящее время является простейшим и удобным средством общения, осуществления платежных операций, просмотра видеоматериалов, развлечения и выполнения множества других действий.

Так как мобильное устройство является неотъемлемой частью жизни человека, важно обеспечить его безопасность. Эксперты отмечают, что наибольшую опасность для мобильного устройства несет, скорее, владелец, чем киберпреступники. У пользователя мобильного устройства гораздо больше шансов потерять его либо данные из него, что является наиболее простым способом для формирования предпосылки по совершению какого-либо противоправного деяния, чем его взлом.

Для обеспечения безопасности мобильного устройства экспертами по мобильной безопасности разработаны следующие рекомендации [1].

1. Пользователю следует включить *автоматическую блокировку экрана*, когда устройство находится в режиме ожидания. Это обстоятельство повышает гарантию защиты от несанкционированного доступа к информации, содержащейся в устройстве, если оно будет потеряно или похищено. Эксперты отмечают, что в большинстве современных мобильных устройств включение блокировки экрана также включает шифрование, помогая защитить данные, хранящиеся на устройстве [1]. Еще одной рекомендацией является защита устройства надежным паролем. К примеру, для разблокировки экрана лучше устанавливать сложный пароль и отказаться от использования графического ключа или PIN-кода. Надежный пароль должен включать буквы в разных регистрах, цифры и прочие знаки [2].

2. Пользователю рекомендуется включать *автоматическое обновление* на своих устройствах. Злоумышленники всегда ищут новые слабые места в программном обеспечении. Постоянное обновление устройств значительно затрудняет их взлом [1; 2].

3. Установка либо включение надежного программного обеспечения для *удаленного отслеживания мобильного устройства* через Интернет. Таким образом пользователь может подключиться к нему через Интернет и узнать его местоположение, если устройство потеряно или похищено. Таким же образом можно удаленно стереть всю важную и конфиденциальную информацию [1; 2].

4. Установка *надежных и проверенных мобильных приложений*. Рекомендуется устанавливать только необходимые программные приложения из надежных источников, например, AppStore, Google Play. Возможна установка приложений с других сайтов, где они не проходят проверку. Однако с большей вероятностью приложения на сторонних ресурсах Интернета могут быть заражены или вредоносны, что может поставить под угрозу конфиденциальность пользователя мобильного устройства. Перед загрузкой следует убедиться, что приложение имеет много положительных отзывов и активно обновляется поставщиком [1; 2].

5. *Включение двухэтапной аутентификации*. Двухфакторная аутентификация — это достаточно надежный способ защиты любых аккаунтов. При ее включении, помимо ввода пароля, от пользователя требуется предоставить временный одноразовый код, который можно получить по СМС или с помощью специальных приложений, устройств. Без данного кода злоумышленник, узнав пароль пользователя, не сможет войти в аккаунт [2].

6. *Настройка параметров конфиденциальности.* Мобильные устройства собирают обширную информацию о пользователе, в связи с чем необходимо тщательно проверять настройки конфиденциальности устройства, включая отслеживание его местоположения, и убедиться, что конфиденциальные уведомления (например, коды подтверждения) не отображаются на экране, когда устройство заблокировано [1].

Кроме того, пользователю необходимо убедиться, что его мобильное устройство *разрешено для использования на рабочем месте*, при выполнении трудовых обязанностей и т. п. На рабочем месте необходимо быть осторожным и отказаться от производства фото- или видеосъемки, которая может содержать конфиденциальную информацию. Сведения, находящиеся даже на защищенном, по мнению пользователя, мобильном устройстве, и при включении надежных параметров конфиденциальности в какой-то момент могут стать общедоступными и, как следствие, повлечь негативные последствия [1].

Соблюдение указанных рекомендаций позволит снизить вероятность утраты информации, содержащейся в памяти мобильных устройств, окажет положительное воздействие на состояние преступности.

1. Beckers J. Securing Your Mobile Devices [Electronic resource] // SANS. URL: https://www.sans.org/newsletters/ouch/securing-mobile-devices/ (date of access: 30.09.2021). Перейти к источнику Вернуться к статье

2. Как защитить Android [Электронный ресурс] // Блог Лаборатории Касперского. URL: https://www.kaspersky.ru/blog/android-maximum-security-tips/5938/ (date of access: 30.09.2021). Перейти к источнику Вернуться к статье